Secure Hash Performance Analysis Report

Date: November 2025

Subject: Performance benchmarking, host-side memory optimization, and overhead analysis of SHA-256 Trusted Application (TA).

1. Critical Issue Resolution: Host Memory Exhaustion

Initial attempts to process large files (e.g., 105 MB) resulted in an **Out of Memory (OOM)** crash on the Host device. This occurred because the original implementation attempted to **malloc()** the entire file size into contiguous RAM before sending it to the TEE.

Issue	Original Behavior	Fixed Behavior
Host Memory Usage	Allocated entire file (e.g., 105 MB) into RAM.	Uses constant 1 MB buffer regardless of file size.
Data Transfer Strategy	Single bulk transfer → crashes for large files.	Streaming 1 MB chunks sequentially → stable for >50

Results:
- Host RAM usage dropped from **105 MB** → **1 MB**.
- Successfully hashed a **52.4 MB** file with linear overhead.
- No further OOM or fragmentation issues observed.

2. Performance Observations

A. The Initialization Floor (Base Cost)

Small file tests (1–100 Bytes) revealed a fixed minimum execution time of **~65–67 µs**, representing unavoidable TEE setup overhead.

Component	Description
Operation Allocation	Creating TA session structures in Secure World
Crypto Context Setup	Initializing SHA-256 secure context
Finalization	Final secure hash computation and cleanup

B. Linear Scalability

For files larger than 4 KB, hashing time increases linearly at approximately **0.08 µs per Byte**. No thermal throttling, caching anomalies, or algorithmic inefficiencies detected.

3. Metric Analysis: Overhead

Metric	Value	Interpretation
Base Initialization Cost	~67 µs	Minimum cost for even 0-byte input
Context Switch Overhead	~1.6 µs	Cost per chunk (1 MB in streaming mode)
Max Throughput	~12.5 MB/s	Peak achievable rate
Hardware Frequency	19.2 MHz	Stable CNTFRQ_EL0 reading

The traditional “Overhead per Byte” metric is misleading for this system because it fluctuates from 1.5 µs/Byte for tiny messages to as low as 0.000001 µs/Byte for large files.

The scientifically correct metric is **Overhead per Operation**, which is constant at **~1.6 µs**. Since streaming mode triggers only one operation per 1 MB chunk, hashing efficiency exceeds **99.9%**.